数理解析研究所講究録
1096 巻 1999 年 25-34

Reverse Mathematics and weak second-order systems of 0-1 strings

Takeshi Yamazaki (山崎　武)

Mathematical Institute, Tohoku University

Abstract. From a standpoint congenial to Reverse Mathematics, we develop a basic part of real analysis within weak second-order systems of 0-1 strings, e.g., **BTFA**. Among others, we show within **BTFA** that a version of the maximum principle is equivalent to Σ_1^b-**CA**.

§1. Introduction.

The purpose of Reverse Mathematics is to determine which set existence axioms are needed to prove a popular theorem of mathematics. For the main-stream researches of this program, the system $\mathbf{RCA_0}$ is presupposed as a base theory in which most of basic concepts of ordinary mathematics (e.g., reals, continuous functions) are defined. However, it has been claimed by several people that the phenomena of Reverse Mathematics depend on the base theory, so that necessary axioms for a theorem may be changing if one replaces $\mathbf{RCA_0}$ by a weaker system. Actually, Simpson and Smith [6] already studied Reverse Mathematics over $\mathbf{RCA_0^*}$, which is roughly $\mathbf{RCA_0}$ minus Σ_1^0-induction plus Σ_0^0-induction plus exponentiation. F.Ferreira [2] proposed to do Reverse Mathematics over **BTFA** (or **BTFA**+Σ_∞^b-WKL), a second-order systems of 0-1 strings whose provably total functions are the polynomial time computable functions.

In this paper, we carry out Ferreira's plan and show, for instance, that the intermediate value theorem on $[0,1]$ is provable in **BTFA**, and a version of the maximum principle is equivalent to Σ_1^b-**CA** within **BTFA**.

In the rest of this section, we quickly review the basic concepts about second-order systems of 0-1 strings following [2]. Then in §2, we develop real analysis within such systems, and in §3, we prove our main results.

The language of second-order systems of 0-1 strings consists of three constant symbols ε, 0, and 1, two binary function symbols $\frown$(for concatenation) and $\times$($x \times y$ means the word x concatenated with itself the length of y times) and a binary relation symbol $\subseteq$ (for initial subwordness). The class of s.w.q. formulae (where s.w.q. stands for "subword quantification") is the smallest class of formulae containing the atomic formulae and closed under the Boolean operations and quantifications of the form $\forall x \subseteq^* t$ or $\exists x \subseteq^* t$ where $x \subseteq^* y$ means $\exists z \subseteq y(z^\frown x \subseteq y)$ and t is a term in which the variable x does not occur. The relation $x \leq y$ is defined by $1 \times x \subseteq 1 \times y$ to express that the length of x is less than or equal to the length of y. We write $1 \times x$ for $|x|$. Σ_1^b-formula is a formula of the form $\exists x \leq t\varphi$ where φ is a s.w.q. formula and t is a term in which the variable x does not occur. The class of Σ_∞^b-formulas is the smallest class containing the s.w.q. formulas and closed under Boolean operations and bounded quantification, i.e., quantification of the form $\exists x \leq t(\ldots)$ or $\forall x \leq t(\ldots)$, where the variable x does not occur in the term t.

Definition 1 i) (\$)-CA *is the set of universal closures of formulas of the form*

$$\forall x(\exists y\varphi(x,y) \leftrightarrow \forall z \neg\psi(x,z)) \rightarrow \exists X \forall x(x \in X \leftrightarrow \exists y\varphi(x,y)),$$

where φ and ψ are Σ_1^b-formulae X does not occur in φ.

ii) Σ_1^b-**CA** *is the set of universal closures of formulas of the form*

$$\exists X \forall x (x \in X \leftrightarrow \varphi(x)),$$

where φ *is* Σ_1^b*-formulae and* X *does not occur in* φ*.*

iii) Σ_1^b-**NI** *(notation induction) is the set of universal closures of formulas:*

$$\varphi(\varepsilon) \wedge \forall x(\varphi(x) \rightarrow \varphi(x0) \wedge \varphi(x1)) \rightarrow \forall x \varphi(x),$$

where φ *is* Σ_1^b*-formula.*

iv) $\mathbf{B}\Sigma_\infty^b$ *is the set of universal closures of formulas:*

$$\forall x \leq a \exists y \varphi(x, y) \rightarrow \exists z \forall x \leq a \exists y \leq z \varphi(x, y),$$

where φ *is* Σ_∞^b*-formula.*

Definition 2 (See [2] for a complete statement) i) Σ_1^b-**NIA** *consists of the axioms for basic word operators* $\frown$, $\times$, *etc. plus* Σ_1^b-**NI**.

ii) BTFA *is* Σ_1^b-**NIA**+$\mathbf{B}\Sigma_\infty^b$+**($)-CA**.

We notice that Σ_1^b-**NIA** and Buss' S_2^1 are mutually interpretable. Originally, **BTFA**, which stands for base theory for feasible analysis, is introduced by F. Ferreira [2] to answer Sieg's problem: find a mathematically significant subsystem of analysis whose class of provably recursive functions consists only of the computationally "feasible" ones. It is obvious that the smallest model of **BTFA** is $(2^\omega, \Delta_1^0)$, though it is unknown whether or not ($)-**CA** implies Σ_1^b-**CA**. The following theorem is a major characterization of systems Σ_1^b-**NIA** and **BTFA**.

Theorem 1 i) Σ_1^b-**NIA**+$\mathbf{B}\Sigma_\infty^b$ *is conservative over* Σ_1^b-**NIA** *with respect to* Π_2^0*-formulas.*

ii) BTFA *is conservative over* Σ_1^b-**NIA**+**B**Σ_∞^b *with respect to* Π_1^1*-formulas.*

For a proof of this theorem and other related results, see Ferreira [2].

§2. Basics of real analysis.

We begin with defining a real number and a (uniformly) continuous function on the reals in **BTFA**. We here have two sorts of natural numbers, i.e., tally natural numbers and dyadic natural numbers. A *tally natural number* is defined by a string of 1's, i.e., ε, 1, 11, ... Let **N** be the set of tally natural numbers. We can define $0_{\mathbf{N}}$, $\leq_{\mathbf{N}}$, $+_{\mathbf{N}}$ and $\cdot_{\mathbf{N}}$ by ε, $\subseteq$, $^\frown$ and $\times$, respectively. Then it is easy to show in **BTFA** that **N** is an ordered semi-ring. We use n, m, l, k, ... as variables over **N**. A tally natural number is used to express the length of a string or the index of a sequence. A string σ is a *dyadic natural number* if $\sigma = 1\tau$ for some τ, or $\sigma = 0$. In the standard model, σ can be seen as the ordinary dyadic notation of a natural number. The set of all dyadic natural numbers is denoted by $\mathbf{N}_2$. Also we can define $0_{\mathbf{N}_2}$, $\leq_{\mathbf{N}_2}$, $+_{\mathbf{N}_2}$ and $\cdot_{\mathbf{N}_2}$ in the usual way (cf. Ferreira [3]), and show in **BTFA** that $\mathbf{N}_2$ is an ordered semi-ring. We should notice that there exists a natural embedding of **N** into $\mathbf{N}_2$, but not vice versa. Without misunderstanding, we omit subscripts of $+_{\mathbf{N}}$, $\leq_{\mathbf{N}_2}$, etc.

A 3-tuple (i, n, σ) denotes a *dyadic rational number* $(-1)^i 2^n \sum \sigma(j) 2^{-j-1}$ where $i = 0$ or 1 and $\sigma(j)$ is the j'th element (0 or 1) of σ. Let D' be the set of dyadic rational numbers. Then we define $=_{D'}$, $\leq_{D'}$, $+_{D'}$, $\cdot_{D'}$, etc. in the usual way. We have a natural embedding of $\mathbf{N}_2$ into $D'/=_{D'}$. Let D be the set of $D' \cap [0,1]$. D_n is the set of all elements $(0, m, \sigma)$ of D where the length of σ is $m + n$.

To simplify the notation, we write σ for $(0, n, 0^n\sigma) \in D$, where 0^n is the string of 0's whose length is n. Moreover, we write 2^{-n} for $0^{n-1}1$.

Definition 3 (BTFA) *A function* $f : \mathbf{N} \to D'$ *is a real number if* $|f(n) - f(m)| \leq 2^{-n}$

for each $n \leq m$. *Two real numbers* f *and* g *are said to be equal if* $\forall n \in \mathbf{N}(|f(n) - g(n)| \leq 2^{-n+1})$.

The relations $<$, $\leq$ and basic operations on the real numbers are defined as usual. Note that $=$, $\leq$ on the real numbers can be defined by a formula of the form $\forall \sigma \varphi(\sigma)$ where φ is Π^b_1.

Definition 4 (BTFA) $F = (\{f_n\}, m)$ *is a (code for a) (uniformly) continuous function from* $[0,1]$ *to* $[0,1]$ *if* F *satisfies the following conditions:*

1. $m : \mathbf{N} \to \mathbf{N}$ *is an increasing function, called a modulus function for* F.
2. $\{f_n\}$ *is a sequence of piecewise linear functions* $f_n : D \to D$ *whose break points are in* $D_{m(n)}$,
3. $|f_n(d) - f_n(d + 2^{-m(n)})| \leq 2^{-n}$ *for each* $n \in \mathbf{N}$ *and* $d \in D$,
4. $|f_n(d) - f_{n+m}(d)| \leq 2^{-n}$ *for each* $n, m \in \mathbf{N}$ *and* $d \in D$.

We define $F(x) = \langle r_n \rangle$ for each $x \in [0,1]$ by **($)-CA**. Namely, if x is not equal to any $\sigma \in D$, then we define $r_n = f_{n+1}(\sigma)$ where σ is the unique string such that $|x - \sigma| \leq 2^{-m(n+1)-1} \wedge \sigma \in D_{m(n+1)}$. If $x = \tau$ for some $\tau \in D$, $r_n = f_{|\tau|+n}(\tau)$.

Remark 1. It is easy to extend the above definition to define a continuous function from any bounded closed interval to any bounded closed interval. Also a multi-dimensional continuous function can be defined in an obvious way. The identity function, the constant function, $+$, $\cdot$, x^n, etc. are all continuous. The continuous functions are closed under the composition.

Remark 2. We could adopt another definition of continuous functions such as given in Simpson [5]. However, with such a definition, we may not compute $F(x)$ even if F has a modulus function (except for a polynomial.)

The following lemma can be used to show that functions defined by power series, e.g., $\exp(x)$ and $\sin(x)$, are continuous on $[0,1]$.

Lemma 2 (BTFA) *Let $\{F_n\}$ be a sequence of continuous functions $F_n : [0,1] \to [0, 2^{-n}]$ with the modulus function m_n. Suppose that there exists $m : \mathbf{N} \to \mathbf{N}$ such that $m_n(k) \leq m(k+n)$ for each $n, k \in \mathbf{N}$. Then $F = \sum_{k\in\mathbf{N}} F_k$ is continuous.*

Proof. We reason in **BTFA**. Let $F_n = (\{f_m^n\}, m_n)$. Let $\sigma\lceil n$ denote the initial segment of σ whose length is n. Since we can compute $\sum_{k=0}^{m} \sigma_k \lceil n$, then we have a continuous function $F = (\{\sum_{k=0}^{n} f_{2n}^k \lceil 2n\}, m)$. □

§3. The intermediate value theorem and the maximum principle.

Before proving the intermediate value theorem, we show a useful lemma.

Lemma 3 (BTFA) *Let g, h_0 and h_1 be functions and t be a term. Assume that there is a term t' such that $g(\tau) \leq t'(\tau)$ for each τ. Then, there exists f such that*

$$f(\varepsilon, \tau) = g(\tau)$$

$$f(\sigma 0, \tau) = h_0(f(\sigma, \tau), \sigma, \tau)\lceil t(\sigma 0, \tau)$$

$$f(\sigma 1, \tau) = h_1(f(\sigma, \tau), \sigma, \tau)\lceil t(\sigma 1, \tau)$$

Proof. By modifying the proof of proposition 7 in Ferreira [1], f is obtained by a formula of the form $\exists y \varphi$ with $\varphi \in \Sigma_1^b$, which just describes the course of values. By **($)-CA**, f exists. □

Theorem 4 (BTFA) *Let F be a continuous function from $[0,1]$ to $[0,1]$ such that $F(0) < 1/2 < F(1)$. Then, there exists a real $x \in (0,1)$ such that $F(x) = 1/2$.*

Proof. We may assume that $F(\sigma) \neq 0$ for all $\sigma \in D$. Then by **($)-CA** there exists a set X consisting of all $\sigma \in D$ such that $F(\sigma) > 0$. By the above lemma, we define

$g : \mathbf{N} \to D$ by

$$g(n) = \begin{cases} 0 & \text{if } n = \varepsilon, \\ g(n-1)0 & \text{if } n \neq \varepsilon \text{ and } g(n-1)1 \in X, \\ g(n-1)1 & \text{otherwise} \end{cases}$$

By Σ_1^b-**NI**,

$$\forall n \in \mathbf{N} \forall m \in \mathbf{N}[n \leq m \to g(n) \subseteq g(m) \wedge g(n) \equiv n+1].$$

Thus g is a real. By Σ_1^b-**NI** again, $\forall n \in \mathbf{N}[F(g(n)) < 1/2 < F(g(n) + 2^{-n})]$. Therefore, $F(x) = 1/2$ where $x = g$. □

If the modulus function for a continuous function F is of the form $|t|$ where t is a term, then we say that F has a polynomial modulus function.

We now prove a lemma saying that a weak version of the maximum principle can be shown in **BTFA** adding a very weak comprehension scheme.

Lemma 5 (BTFA+Σ_1^b-CA) *For each continuous function F on $[0,1]$ with a polynomial modulus function, then there exists* $\sup_{0 \leq y \leq 1} F(y)$.

Proof. Let $F = (\{f_n\}, m)$. By Σ_1^b-**CA**, there is $X_n^l = \{\tau \lceil l : \exists \sigma \in D_{m(n)} f_n(\sigma) = \tau\}$.

We define $\varphi(l, n, \sigma)$ by

$$\sigma \in X_n^l \wedge \sigma \equiv l \wedge \forall \sigma' \equiv l(\sigma' < \sigma \to \sigma' \notin X_n^l).$$

Since φ is Π_1^b, we can show that $\forall n \in \mathbf{N} \forall l \in \mathbf{N} \exists! \sigma \varphi(l, n, \sigma)$ by Π_1^b-**NI** on l. Let $g(n) = \sigma$ such that $\varphi(n+2, n+2, \sigma)$. Then, for each $n \in \mathbf{N}$,

$f_{n+2}(d) \leq g(n) + 2^{-n-2}$ for each $d \in D_{m(n+2)}$.

$f_{n+2}(d') \lceil (n+2) = g(n)$ for some $d' \in D_{m(n+2)}$.

Therefore, we can show that g is a real and that g is the least upper bound. □

Corollary 6 (BTFA+Σ_1^b-CA) *For each continuous function F on $[0,1] \times [0,1]$ with a polynomial modulus function, then there exists a continuous function $G(x) = \sup_{0 \le y \le 1} F(x,y)$.*

Proof. It is straightforward from the proof of the above lemma. □

Corollary 7 (BTFA+Σ_1^b-CA) *For each continuous function F on $[0,1]$ with a polynomial modulus function, then there exists a continuous function $G(x) = \sup_{0 \le y \le x} F(y)$.*

Proof. We define a continuous function F' on $[0,1] \times [0,1]$ by

$$F'(x) = \begin{cases} F(0) & \text{if } x < y, \\ F(x-y) & \text{if } y \le x. \end{cases}$$

Then F' has a polynomial modulus function. By the above lemma, we can obtain a continuous function $G(x) = \sup_{0 \le y \le x} F(y)$. □

Theorem 8 (BTFA) *The following are equivalent:*

1. Σ_1^b-**CA.**

2. *For each continuous function F on $[0,1]$ with a polynomial modulus function, then there exists a continuous function $G(x) = \sup_{0 \le y \le x} F(y)$.*

Proof. The implication from 1 to 2 is Corollary 7. It remains to prove that 2 implies 1. We reason in **BTFA**.

Let $\varphi(\sigma)$ be Σ_1^b. For simplicity, we assume $\varphi(\sigma)$ is of the form $\exists \tau \equiv t(\sigma)\psi(\sigma,\tau)$ where $\psi(\sigma,\tau)$ is a s.w.q. formula. (It is a routine to extend the following argument to the general case.)

For each $n \in \mathbf{N}$, let $a_n = 1 - 2^{-n} \in D$. (Namely, $a_n = n$ in the sense of strings.) If σ is the length of n, then let $u_\sigma = a_n + 0^{n+1}s$ and $v_\sigma = u_\sigma + 2^{-2n-1}$. If τ is the length of $|t(n)|$, $y_{\sigma,\tau} = u_\sigma + 0^{2n+2}\tau$ and $z_{\sigma,\tau} = y_{\sigma,\tau} + 2^{-2n-2-|t(n)|}$.

Define a function $H : [0,1] \to [0,1]$ by

$$H(x) = \begin{cases} 2x & \text{if } 0 \le x \le 1/2, \\ 2 - 2x & \text{if } 1/2 \le x. \end{cases}$$

Now we define a continuous function $F = (\{f_n\}, m)$. Let $m(n) = |t(n)| + 2n + 3$. Let $f_n(\sigma) = f_{n-1}(\sigma)$ for $\sigma \le a_n$, $f(\sigma) = a_{n+1}$ for $\sigma \ge a_{n+1}$, and for $\sigma \in [a_n, a_{n+1}]$,

$$f_n(\sigma) = \begin{cases} 2\sigma - v_\sigma & \text{if } \sigma \in [\frac{u_\sigma + v_\sigma}{2}, v_\sigma], \\ u_\sigma & \text{if } \sigma \in [y_{\sigma,\tau}, z_{\sigma,\tau}] \text{ and } \neg\psi(\sigma,\tau), \\ u_\sigma + 2^{-|t(n)|-2n-2} h(2^{|t(n)|+2n+2} \cdot (\sigma - y_{\sigma,\tau})) & \text{if } \sigma \in [y_{\sigma,\tau}, z_{\sigma,\tau}] \text{ and } \psi(\sigma,\tau). \end{cases}$$

If $G(x) = \sup_{0 \le y \le x} F(y)$, then it is easy to see that $\exists \tau \le t(\sigma) \psi(\sigma,\tau)$ iff $G(\frac{u_\sigma + v_\sigma}{2}) - 2^{-|t(\sigma)|-2\cdot|\sigma|-3} > u_\sigma$ iff $g_{|t(\sigma)|+2\cdot|\sigma|+5}(\frac{u_\sigma + v_\sigma}{2}) > u_\sigma$, where $G = (\{g_n\}, m')$. Therefore, there exists $X = \{\sigma : \varphi(\sigma)\}$. □

Note. The above theorem can be viewed as a formalized version of theorem 3.7 in Ko's book [4].

参考文献

[1] F. Ferreira, Polynomial time computable arithmetic, Contemporary Mathematics, Vol. 106, 1990, 137–156.

[2] F. Ferreira, A feasible theory for analysis, J. Symb. Logic, Vol. 59, No. 3, 1994, 1001–1011.

[3] F. Ferreira, Some notes on subword quantification and induction thereof, Logic and algebra, Lecture notes in pure and appl. math., Vol. 180, No1996, 477–489.

[4] K. Ko, Complexity Theory of Real Functions, Birkhäuser, 1991.

[5] S. G. Simpson, Subsystems of Second Order Arithmetic, Springer-Verlag, 1998.

[6] S. G. Simpson and R. Smith, Factorization of polynomials and Σ_1^0 induction, Annals of Pure and Appl. Logic, vol 31,1986, 289–306.